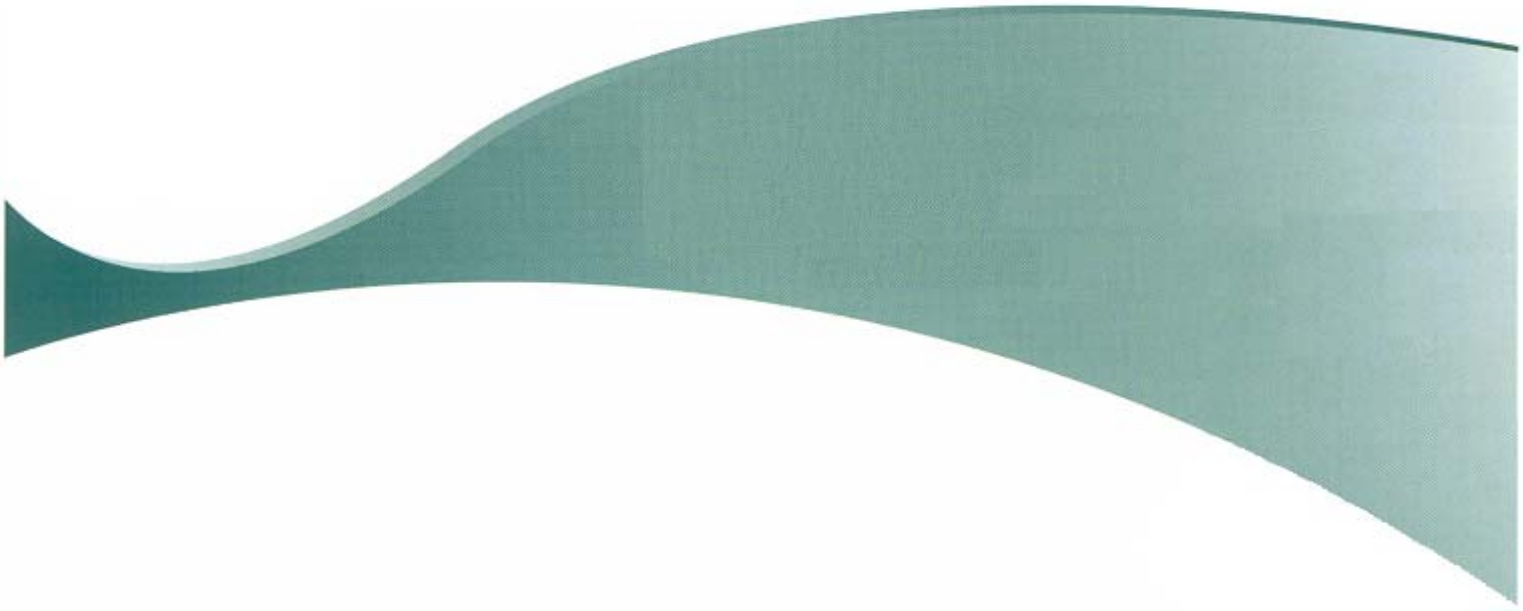
Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

Remote Access Policy



Version 3.0

This policy maybe updated at anytime (without notice) to ensure changes to the HSE's organisation structure and/or business practices are properly reflected in the policy. Please ensure you check the HSE intranet for the most up to date version of this policy

http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/

Reader Information

Title:	HSE Remote Access Policy.
Purpose:	To define a standard for the remote connection to the HSE network.
Author:	Information Security Project Board (ISPB) on behalf of the HSE.
Publication date:	February 2013
Target Audience:	All HSE staff, students, contractors, sub-contractors, agency staff and authorized third party commercial service providers that connect to the HSE network from a remote location.
Superseded Documents:	All local remote access policies and procedures.
Related Documents:	HSE Information Security Policy. HSE I.T. Acceptable Use Policy. HSE Access Control Policy. HSE Third Party Network Access Agreement. HSE Electronic Communications Policy.
Review Date:	February 2014
Contact Details:	Chris Meehan ICT Directorate, Dr.Steevens Hospital Steevens Lane Dublin 8 Email: chris.meehan@hse.ie

Document History

Version	Owner	Author	Publish Date
1.0	HSE	Information Security Project Board (ISPB)	April 2010
2.0	HSE	Information Security Project Board (ISPB)	November 2010
3.0	HSE	Information Security Project Board (ISPB)	February 2013

1.0 Purpose

We live in a time where our workforce is becoming more mobile and the demands for remote access to our network and information systems from our employees, customers and third parties is on the increase. This demand for remote access also comes at a time of increased threats to these resources. In order to ensure the continued security of these I.T. resources we must ensure that we monitor and strictly control all forms of remote access. The purpose of this policy is to define secure standards for connecting to the HSE network from a computer or device located outside of the HSE network.

This policy is mandatory and by accessing any Information Technology (IT) resources which are owned or leased by the HSE, users are agreeing to abide by the terms of this policy.

2.0 Scope

This policy represents the HSE's national position and takes precedence over all other relevant policies which are developed at a local level. The policy applies to:

- All remote connections to the HSE network (LAN/WAN/WiFi);
- All HSE staff, students, contractors, sub-contractors, agency staff and authorized third party commercial service providers that connect to the HSE network from a remote location.

3.0 Definitions

A list of terms used throughout this policy are defined in *appendix A.*

4.0 Policy

4.1 Principles of Remote Access

- Remote access connections must be strictly controlled and only granted to users that meet at least one of the following criteria:

    1) HSE staff, students, contractors, sub-contractors or agency staff who have been approved by the HSE to work from home (Home Workers).

    2) HSE staff, students, contractors, sub-contractors or agency staff whose role requires them to spend a considerable amount of their time out of the office or workplace.

3) HSE staff, students, contractors, sub-contractors or agency staff who are responsible for administration, support or maintenance of the HSE network and/or information systems.

4) Third party commercial service providers who are contracted by the HSE to provide goods and services (for example: technical support, consultancy etc).

- Remote access requests from HSE staff, students, contractors, sub-contractors or agency staff must be reviewed and approved by their Line Manager (at Grade 8 level or higher) to ensure the employee meets the appropriate criteria (as above). HSE staff, students, contractors, sub-contractors or agency staff must only be granted access to network facilities, services and information systems which are necessary for the employee to carry out the responsibilities of their role or function.

- Third party commercial service provider access requests must be sponsored by a HSE information owner (at HSE National Director level (or equivalent)) or his/her nominee (at grade 8 level or higher).

- Remote user's access rights and privileges will be restricted to the minimum services and functions as is necessary for them to carry out their HSE role.

- The ICT Directorate on behalf of the HSE reserves the right to block a remote access request on technical, operational or security grounds.

- All confidential and restricted information transmitted via a remote access connection must be encrypted prior to transmission or sent through an encrypted tunnel, except for where the remote connection forms a direct part of the HSE network.

- Remote access connections must only be used for approved HSE business purposes.

4.2 Remote Access Registration & Management

- All requests for remote access must be made in writing using the ***HSE Remote Access Request Form*** *(http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Forms/Remote_Access_Request_Form.pdf).*

- Line managers (at Grade 8 level (or equivalent) or higher) must complete the request on behalf of their staff and forward this onto ICT Directorate.

- Remote access accounts will be created for an initial 6 month period and reviewed and monitored in accordance with the ***HSE Access Control Policy*** (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Access_Control_Policy.pdf*).

- All passwords used to access remote access connections must be created and managed in accordance with the ***HSE password Standards Policy*** ***(****http://hsenet.hse.ie/Intranet/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Password_Standards_Policy.pdf*).

4.3 Third Party Remote Access Registration & Management

- Where there is a business need and with the approval of a HSE information owner or his/her nominee, third party commercial service providers maybe granted access to the HSE network and information systems.

- Third party commercial service provider access requests must be made in writing using the ***HSE Third Party Access Request Form*** **(***http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Forms/Third_Party_Access_Request_Form.pdf***).**

- The information owner or his/her nominee must complete the request on behalf of the third party commercial service provider and forward it to the ICT Directorate along with the following documents:

    1) A copy of the ***HSE Third Party Network Access Agreement*** signed by the third party commercial service provider (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Third_Party_Network_Access_Agreement.pdf*)

    2) A copy of the ***HSE Service Provider Confidentiality Agreement*** signed by the third party commercial service provider (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Service_Provider_Confidentiality_Agreement.pdf*)

- Under no circumstances will third party commercial service provider be granted remote access to the HSE network and information systems until the ICT directorate has received the appropriate documentation.

- Third party commercial service provider remote access accounts will only be granted read/execute privileges by default. Third party commercial service provider maybe granted temporary write privileges which will allow them to amend or update systems. In such circumstances the information owner or his/her

nominee must email the ICT Directorate requesting a change to the third party commercial service provider access privileges for a stipulated period.

- For security reasons all third party commercial service provider remote access accounts except those providing 24*7 support will be switched off (de-activated) by default. Third party commercial service provider will be required to email (can be followed by phone) the ICT Directorate requesting that their account be switched-on (activated) for a stipulated period.

- Third party commercial service provider remote access accounts providing 24*7 support will remain open at all times for diagnostic purposes. However the third party commercial service provider will be required to email the ICT Directorate each time the account is used.

- Third party commercial service provider remote access accounts will be created for an initial 3 month period and reviewed and monitored in accordance with the ***HSE Access Control Policy*** (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Access_Control_Policy.pdf*).

4.4 Remote Access Computer Devices

- All HSE employees connecting to the HSE network remotely must do so using a HSE owned computer device (for example desktop, laptop, mobile computer device etc).

- All computer devices that are connected to the HSE network remotely must have up to date anti-virus software installed.

- Third party commercial service provider computer devices must be used in accordance with the terms of the ***Third Party Network Access Agreement*** (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Third_Party_Network_Access_Agreement.pdf*)

- Where possible confidential and restricted information must not be stored on a remote computer device. In circumstances where it has been deemed necessary and approved by a HSE line manger (at grade 8 level (or equivalent) or above) the information may be stored on a remote computer device provided it is encrypted in accordance with the ***HSE Encryption Policy*** (*http://hsenet.hse.ie/Intranet/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/HSE_Encryption_Policy.pdf*).

4.5 Remote Access Sessions

- Where technically feasible:

    1) Remote access users must be forced to change their password at their first logon. Where this is not possible, users must be instructed to manually change their password the first time they logon using their remote access connection.

    2) All remote access sessions which are inactive for more than 30 minutes must be automatically 'locked' or logged out. Where this is not possible, users must be instructed to manually log off or 'lock' their HSE computer device (using *Ctrl+Alt+Delete* keys) when they have to leave it unattended for any period of time.

    3) All remote access sessions must be monitored and logged.

5.0 Roles & Responsibilities

5.1 ICT Directorate

The ICT Directorate is responsible for:

- The selection, implementation and management of all remote access technologies used within the HSE.
- The management and administration of all HSE remote access accounts.
- The management and administration of all remote access connections to the HSE network.
- The management & implementation of appropriate network security controls
- Monitoring all third party activity while connected to the HSE network.
- The provision and management of anti virus/spyware software throughout the HSE.
- The provision of training, advice and guidance on the use of remote access facilities within the HSE;

5.2 Information Owners

Information owners are responsible for:

- The implementation of this policy and all other relevant policies within the HSE directorate or service they manage;

- The ownership, management, control and security of the information processed by their directorate or service on behalf of the HSE;

- The ownership, management, control and security of HSE information systems used by their directorate or service to process information on behalf of the HSE;

- Maintaining a list of HSE information systems and applications which are managed and controlled by their directorate or service.

- Making sure adequate procedures are implemented within their directorate or service, so as to ensure all HSE employees, third parties and others that report to them are made aware of, and are instructed to comply with this policy and all other relevant policies;

- Making sure adequate procedures are implemented within their directorate or service to ensure compliance of this policy and all other relevant policies.

5.3 Users

Each user is responsible for:

- Complying with the terms of this policy and all other relevant HSE policies, procedures, regulations and applicable legislation;

- Ensuring they only use remote access accounts and passwords which have been assigned to them;

- Ensuring all remote access account passwords assigned to them are kept confidential at all times and not shared with others;

- Changing their passwords at least every 90 days or when instructed to do so by designated system administrators, network administrators or the ICT Directorate;

- Respecting and protecting the privacy and confidentiality of the information they process at all times;

- Ensuring they use their remote access connection in a lawful and ethical manner at all times;

- Complying with instructions issued by the ICT Directorate on behalf of the HSE;

- Reporting all misuse and breaches of this policy to their line manager.

5.4 Line Managers

In addition to each user's responsibilities, line managers are directly responsible for:

- The implementation of this policy and all other related HSE policies within the business areas for which they are responsible;
- Ensuring that all HSE employees who report to them are made aware of and are instructed to comply with this policy and all other relevant HSE policies;
- Ensuring that each user they approve for remote access fulfills the appropriate criteria;
- Consulting with the HR Directorate in relation to the appropriate procedures to follow when a breach of this policy has occurred.

6.0 Enforcement

- The HSE reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. HSE staff, students, contractors, sub-contractors or agency staff who breach this policy maybe subject to disciplinary action, including suspension and dismissal as provided for in the HSE disciplinary procedure.
- Breaches of this policy by a third party commercial service providers, may lead to the withdrawal of HSE information technology resources to that third party commercial service provider and/or the cancellation of any contract(s) between the HSE and the third party commercial service provider.
- The HSE will refer any use of its I.T. resources for illegal activities to the Gardai..

7.0 Review & Update

This policy will be reviewed and updated annually or more frequently if necessary, to ensure that any changes to the HSE's organisation structure and business practices are properly reflected in the policy.

The most up to date version of this policy is published on the intranet at – (*http://hsenet.hse.ie/HSE_Central/Commercial_and_Support_Services/ICT/Policies_and_Procedures/Policies/*).

Appendix A

Authorisation / Authorised: Official HSE approval and permission to perform a particular task.

Backup: The process of taking copies of important files and other information stored on a computer to ensure they will be preserved in case of equipment failure or loss/theft etc.

Confidential Information: Information that is given to HSE in confidence and/or is not publicly known. The Information must only be accessible to those person(s) who are authorised to have access. For example – unpublished financial reports, tenders, contracts, unpublished research material, passwords etc.

Information: Any data in an electronic format that is capable of being processed or has already been processed.

Information Owner: The individual responsible for the management of a HSE directorate or service (HSE National Director **(**or equivalent)).

Information System: A computerized system or application used to access, record, store, gather and process information.

Information Technology (I.T.) resources: Includes all computer facilities and devices, networks and data communications infrastructure, telecommunications systems and equipment, internet/intranet and email facilities, software, information systems and applications, account usernames and passwords, and information and data that are owned or leased by the HSE.

Line manager: The individual a user reports directly to.

HSE Network: The data communication system that interconnects different HSE Local Area Networks (LAN) and Wide Area Networks (WAN).

Password: A string of characters that a user must supply in order to gain access to an IT resource.

Personal Information: Information relating to a living individual (i.e. HSE employee, client or patient) who is or can be identified either from the Information or from the information in conjunction with other information. For example: - an individuals name, address, email address, photograph, date of birth, fingerprint, racial or ethnic origin, physical or mental health, sexual life, religious or philosophical beliefs, trade union membership, political views, criminal convictions etc.

Remote Access: Any Connection to the HSE network(s) or information systems that originates from a computer or device located outside of the HSE network.

Third Party Commercial Service Provider: Any individual or commercial company that have been contracted by the HSE to provide goods and/or services (for example, project / contract management, consultancy, information system development and/or support, supply and/or support of computer software / hardware, equipment maintenance, data management services, patient / client care and management services etc.) to the HSE.

Users: Any individual using a HSE's remote access account or any other HSE IT resource.